# Vodafone Group Plc

## Cyber Security Factsheet 2024

# Introduction

Our role is to enable connectivity in society. As a provider of critical national infrastructure and connectivity that is relied upon by millions of customers, we prioritise cyber and information security across everything we do.

Cyber attacks are part of all our lives today and will be in the future. All organisations, governments and people will be subject to cyber attacks and some will be successful. The telecommunications industry is faced with a unique set of risks as we provide connectivity services and handle communication data. Our operating model and strategy are designed based on this threat landscape, and we implement controls that prevent, detect and respond to attacks to minimise impact.

This factsheet provides detail on our approach to managing cyber risk at Vodafone, as well as how we protect our customers from cyber threats. Our cyber security strategy is aligned to the Company's strategy and focused on the actions we need to take to protect our customers and society now and in the future.

### Videos

Scan or click to watch our Chair talk about the importance of cyber security during his Board site visit:
**investors.vodafone.com/videos**

Scan or click to watch our Group Chief Executive talk about the importance of cyber security:
**investors.vodafone.com/videos**

# Contents


**Strategy**

02 Our cyber security strategy
02 Customers
03 New technologies, industry collaboration

**Risk management**

04 Identification of vulnerabilities and risks
04 Risk and control approach

**Our operating model**

06 Our approach to cyber security
07 Governance

**Culture, training and awareness**

08 Training and awareness
08 Growing our skills
08 The Cyber Code

**Threats and incidents**

09 Threat landscape and intelligence
09 Cyber operations and incidents

**Compliance**

10 Securities and Exchange Commission cyber security disclosure requirements


# Highlights

**Our vision** — a secure connected future for our customers and society

**Global scale** — through consistent cyber security baseline, global telemetry and deep expertise

**900 employees** — in-house international team of experts

**9 million** — consumers and businesses use our cyber security solutions to protect themselves

**ISO 27001 certified** — across our global technology function and 11[1] local markets

**Independent testing** — of our mobile networks every year

**Mandatory cyber training** — with cyber incident simulations run leadership teams

**Contribution to UN Sustainable Development Goals ('SDGs')**

Note:
1. Excludes Vodafone Italy and Vodafone Spain.

# Strategy

## Our cyber security strategy

Our vision is a secure connected future for our customers and society. We are motivated by a clear purpose to inspire customer trust and loyalty by providing sustained cyber security, ultimately contributing to a secure society and an inclusive future for all.

Our cyber security strategy and operating model support our vision and goals, and form part of our wider Company strategy. Each year we refresh our cyber security strategy and every five years redevelop the cyber security strategy based on changes in the internal and external environment.

Our strategy is based on core principles, including:

- Act as an enabler for the business;
- Be proactive, risk and threat-led, supported by data-driven decisions, automation and digitalisation;
- Build and assure security in all products and services; and
- Simplify architecture though partnership with key suppliers.

To implement these principles, our strategy is delivered through six pillars of change:

**Control evolution:** Maintain and improve our security controls and procedures beyond the existing cyber security baseline with an adaptive and risk-based framework.

**Secure by design:**
All products and services have security built-in whether we build them ourselves or buy them from vendors.

**Dynamic trust:** Strong zero-trust security based on dynamic risk-based access that is frictionless for users, for example, multi-factor authentication and moving away from passwords.

**Real-time data, real-time response:** The next generation of our detection and response capability, more automated and based on advanced analytics.

**Spirit of Vodafone & cyber culture:** The next generation of our detection and response capability, more automated and based on advanced analytics.

**Security for society:** Collaborate widely to encourage standardisation, share intelligence, and engage on regulation.

Each year we define and communicate priorities for a three-year period, so all areas of our business are clear on the investment priorities for security. We track progress against these priorities throughout the year.

### Strategic pillars

### Year ahead

The priorities for the coming year include updating and redeveloping our cyber security strategy in line with future technology changes and expected threats. This strategy will position us to manage changes in technology, threats and the external environment.

Key priorities for the year include:

- Design and development of a new security operations platform;
- Further strengthening of identity, access control and authentication;
- End-to-end security of our telecommunications networks, transforming how we manage the security of our third parties; and
- New adaptive cyber risk methodology.

Alongside these shifts, we continue to focus on security control improvement, efficiency and automation, including automation of key risk indicators that provide data driven measurement of our security position.

## Cyber security products & services for our customers

We provide cyber security support to our customers through Vodafone Consumer and Vodafone Business.

For Consumers, we offer our Secure Net service to help keep them and their families safe. Secure Net detects and protects against online malware, infections and viruses, provides smart alerts if a customers' identity is compromised, and provides parents with advanced parental controls. At the end of March 2024, Secure Net was available to mobile customers in 7 markets and converged customers in 4 markets and had nearly 8 million subscribers. Where Consumers subscribe to additional security products, such as Secure Net, there are also significant NPS benefits.

We also provide cyber security support to our business customers through Vodafone Business. Our products and services help our business customers of all sizes protect themselves from the evolving cyber security threat landscape and adapt to a new model of security necessitated by the adoption of hybrid working. Our portfolio of cyber security solutions for businesses is available in 16 markets and has nearly 1 million users. Our products and services leverage our global network and partnerships, such as those with Accenture, Lookout, Trend Micro, and VMWare, to make enterprise-grade security services accessible to organisations of any size.

For SOHO and SME customers our focus is on click-to-buy services covering endpoint and network security, as well as risk assessments and cyber training. In the coming year, we are expanding our comprehensive portfolio to include backup, secure connectivity and external risk protection services.

For mid-market business customers, we offer a range of professional and managed services that provide support across the full spectrum of an organisation's cyber security needs – assessing risk with vulnerability assessments; penetration testing and cyber exposure diagnostics; protecting the organisation with firewall management and phishing awareness campaigns; through to full scale managed detection and response, and breach response and forensics services.

For larger and multinational organisations, Vodafone Business offers a range of network, endpoint and managed security solutions to enhance mobile and fixed portfolios in this segment.

Click to read more about our strategic partnerships on page 11 of our FY24 Annual Report: **vodafone.com/ar2024**

# Strategy continued

## New technologies and industry collaboration

We adopt new technologies to better serve our customers and gain operational efficiency. For every technology programme, new or existing, we follow our Secure by Design process, evaluating suppliers' hardware and software, modelling threats and understanding the risks before designing, implementing and testing the necessary security controls and procedures.

### Mobile networks

Every new mobile network generation has brought increased performance and capability, along with new opportunities in security. As we deploy 5G core networks alongside our 5G radio networks, often described as 5G Standalone, we have updated our security standards to implement the latest 5G features in our core networks. We also test security in our radio networks using independent third-party testing companies.

OpenRAN is a new way of building and managing radio access network ('RAN') components within telecommunication infrastructure. Instead of purchasing all the components from one supplier, we use hardware and software components from multiple vendors and integrate these via open interfaces. Over time, this will create a more competitive landscape for telecommunications equipment. We continue to collaborate with other players in the OpenRAN ecosystem to improve security. This includes adding requirements to the OpenRAN specification, publishing internal security standards, and benchmarking vendors against these. The first OpenRAN sites are now live in the UK, Romania and DRC.

### Artificial Intelligence

We take the responsible use of AI seriously and seek to balance the opportunities and risks associated with AI, and more recently generative AI ('Gen AI'). Teams from across the business are collaborating under the governance of a global AI governance board which agrees policy, mitigates threats, identifies and selects use cases for implementation.

Click to read more about AI governance on page 46 of our FY24 Annual Report: **vodafone.com/ar2024**

We are experimenting with public and private Large Language Models ('LLMs') to support a range of potential business cases. To date, two private versions of models have been reviewed and approved though our Secure by Design process. To reduce the risks of misuse, we limit access to specific public LLMs. We have developed an awareness programme and updated our guidance and policies to make it clear to our employees what data must not be shared in a public AI model.

We have defined requirements for internal LLM application development including risk assessment, designing for transparency, lack of bias and providing the right degree of human oversight of results. If the AI model could have a high impact on people, we require a human to have input on the final decision.

We are also investigating the use of AI to augment our cyber security processes. The first proof of concept is a cyber security chatbot which can answer employee questions on cyber policies and standards. We are also part of cross-industry forums which collaborate on telecommunication-specific AI use cases, including threat detection, investigation and response.

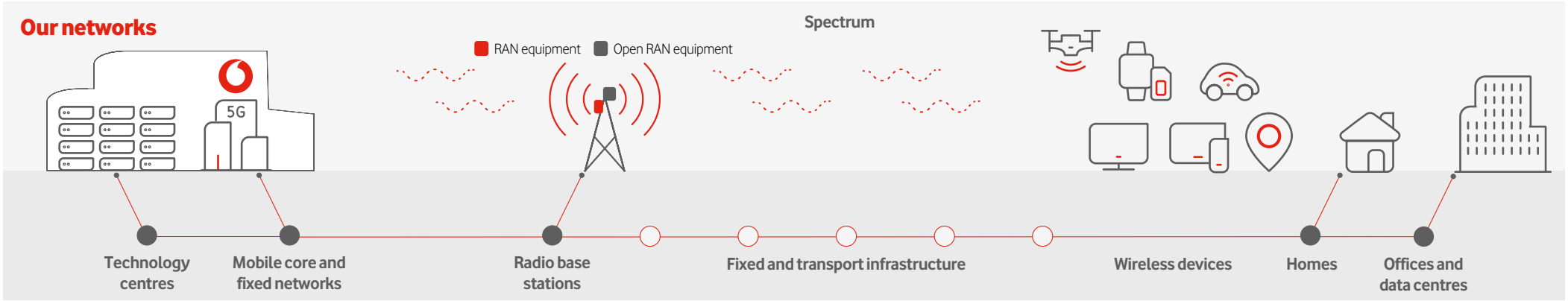
### Quantum computing

We are preparing for a time when quantum computing is available at scale. Through our joint research with IBM, we have developed a risk-based approach to mitigate the risks of existing cryptography, which could be more easily broken by a quantum computer. We are identifying potential quantum vulnerabilities, defining supplier requirements and developing the ability to update our cryptography when new threats emerge. Vodafone also co-chairs the telecommunications industry-wide task force on this issue.

### Industry collaboration

We actively engage with stakeholders across industry, with regulators, standard-setting bodies and governments. Collaboration is vital to respond to threats, protect our organisation and workforce, and build safe online and digital spaces for customers and society. We use our expertise and experience to engage with a wide range of organisations to help improve the understanding of cyber security thinking and practice, and contribute to public policy, technical standards, information sharing, risk assessment, and governance. For example, we have engaged in cross-industry collaboration through the European Round Table, where we chair the CISO committee. We have an appointed member on the National Cyber Advisory Board in the UK. We also collaborate with other telecommunication companies, and actively engage in security standards working groups such as ENISA 5G Cyber Security Certification, O-RAN Alliance Security Focus Group and GSMA Fraud and Security Group.

## Our networks



# Risk management

## Identification of vulnerabilities and risks

Cyber attacks are part of the technology landscape today and will be in the future. All organisations, governments and people will be subject to cyber attacks and some will be successful, leading to security incidents. The telecommunications industry is faced with a unique set of risks as we provide connectivity services and handle private communication data.

As a result, cyber security is one of Vodafone's principal risks. A successful cyber attack could cause serious harm to the Company or its customers, including unavailability of services or a data breach leading to disclosure or misuse of customer personal data. The consequences could include, but are not limited to, exposure to contractual liability, litigation, regulatory action, or damage to the company's reputation and brand and loss of market share. In the worst case, the cyber security incident could cause material financial impact to the Company.

There is increasing regulatory focus on cyber security and requirements for telecommunications providers to improve their cyber security practices. The Company is subject to GDPR and equivalent legislation in many countries in which it operates. In addition, there are cyber focused local laws and regulations, for example in the UK with the Telecoms Security Act. A cyber incident may therefore lead to regulatory fines and other enforcement activities if deemed to be due to inadequate security. Measures to meet these laws and regulations will also result in increased compliance costs.

We dedicate significant resources to reducing cyber security risks, however due to the nature of the threats, we cannot provide absolute security and some cyber security incidents will occur.

Risk and threat management are fundamental to maintaining the security of our services across every aspect of our business. We separate cyber security risk into three main areas of risk:

- **External:** A wide variety of attackers, including criminals and statebacked groups, target our networks, systems and people using a range of techniques and procedures. They seek to gain unauthorised access to steal or manipulate data or disrupt our services.
- **Insider:** Our employees may accidentally leak information or maliciously misuse their privileges to steal confidential data or to cause disruption; and
- **Supply chain:** We only have indirect control over the cyber security of third-party service providers, limiting our ability to defend against cyber threats to these third parties. Such attacks, if successful, could cause services to be unavailable or enable a data breach to occur.

To help us identify and manage emerging and evolving risks, we constantly evaluate and challenge our business strategy, new technologies, government policies and regulation, and cyber threats.

We conduct regular reviews of the most significant security risks affecting our business and develop strategies and policies to detect, prevent and respond to them. Our cyber security strategy focuses on minimising the risk of cyber incidents that affect our networks and services. When incidents do occur, we identify the root causes and use them to improve our controls and procedures.

Cyber security risk is aligned with Vodafone's enterprise risk framework. Each principal risk owner is responsible to produce a formal Line of Sight document twice a year that describes the risk, the Company's risk tolerance, current position, control position and actions to move to tolerance if required. Second and third line assurance supporting the report is also included in the Line of Sight document.

Hackers can exploit a wider attack surface than ever before

# Risk management continued

## Risk and control approach

The global Cyber and Information Security policy applies to all Vodafone-controlled entities. Each security domain has a more detailed supporting policy document with detailed control objectives. The policies are underpinned by security standards which provide relevant technical specifications.

### Control framework

Security controls and procedures define the requirements which allow our policies to be met. These controls and procedures are designed to prevent, detect or respond to threats. Most risks and threats are prevented from occurring and we expect most will be detected before they cause harm and need a response.

We have defined a common global control framework called the Cyber Security Baseline ('CSB') and adoption is mandatory across the entire Group. We based the CSB on the ISO 27001 international standard, mapping those controls to our cyber risks to identify the most impactful. Our original baseline included 48 key controls, this has grown to 56 as we have reviewed and identified new controls to counter new cyber threats.

All controls in the baseline need to be effective in all entities. We define effectiveness based on the depth of the control implementation and coverage of the relevant assets. We understand that cyber security controls need to be continuously evolved and enhanced to mitigate risks and threats. Each year we set new annual targets, and progress against the targets is monitored and reported to the senior leadership team in each market and the technology leadership team quarterly. We update our priorities with changes, including any necessary new controls and procedures.

In addition to this top-down process of risk identification and mitigation, we identify individual cyber risks at the product or system level, for example through our Secure by Design process, operational activities, scanning and monitoring, or through an incident. Risks are evaluated on a common impact and likelihood scale, mitigating actions are agreed and captured in a risk register. Any high risks identified through these processes require senior management oversight and agreement of mitigating actions.

### Adaptive Risk and Control Methodology

A risk and control methodology is important to drive action in any company. We are launching a new global methodology for cyber security risk management, which was developed with the assistance of a major consulting firms. During FY25 we will retire the CSB and replace it with the new methodology. This methodology has a greater focus on risk and threats but retains the structured control framework and common targets of CSB. Controls are vital to reduce risk and initially we will continue to use the same control set under the new methodology. To adapt to the changing threat landscape, the new methodology introduces threat and risk scenarios. The threats and specific attack techniques are mapped to the controls that most significantly reduce risk, allowing gaps to be highlighted. The control framework will continue to evolve based on technology changes, our strategic and business priorities, and changing regulation.

Over the next three years, we intend to automate the capture and reporting of key risk indicator data from source systems. This will reduce manual effort, be more accurate and provide stronger assurance of effectiveness. Further, to better quantify residual risk, we have also created a risk quantification model based on threats, control effectiveness and incident data. This will be tested and launched during FY25.

Click to read more about our identification of cyber threat as a principal risk on page 60 of our FY24 Annual Report: **vodafone.com/ar2024**

### Assurance

A dedicated technology assurance team review and validate the effectiveness of our cyber security controls and procedures, and our control environment is subject to regular internal audit. We test the security of our mobile networks every year using a specialist testing company, they also benchmark our security against other telecommunications operators. This provides assurance that we are maintaining the highest standards and our telecommunications controls are operating effectively. We have also appointed external specialists to perform testing on our security controls ('red teaming') to uncover any areas for improvement. We maintain externally audited information security certifications, including ISO 27001, which cover our global technology function and 11 local markets. In addition, our markets comply with national information security requirements where applicable. All systems going live and those undergoing change are independently penetration tested. An internal team performs some testing, and we engage third party testers where appropriate. Across Vodafone, we complete over 1,000[1] penetration tests every year. We also perform adversary testing exercises using independent third parties.

### Supply chain

As well as monitoring control effectiveness within Vodafone, we oversee the cyber security of our suppliers and third parties. Controls and procedures are embedded in the supplier lifecycle to set requirements, assess the risk and monitor each supplier's security performance. At supplier onboarding, minimum security requirements are written into contracts, and we determine the inherent risk of the supplier based on the service they are providing. We then assess their controls and procedures using a questionnaire to understand the residual risk, which informs the frequency of review from annual to every three years. We follow up on open actions and ensure any security incidents are tracked and managed.

### Regulatory landscape

We expect a continued increase in security regulation over the next few years as governments respond to the heightened cyber threat landscape, recognising that telecommunications operators provide critical national infrastructure. We engage directly with governments and industry partners to promote proportionate, risk-based and cost-effective solutions to security threats. We look to establish shared approaches to reinforce standardisation and regulatory frameworks that apply equally to all market participants.

In the UK, we are implementing the provisions of the Telecommunications Security Act which sets enhanced security requirements for UK network operators and their suppliers. In Europe, individual member states have their own current or pending legislation, which incorporate EU-wide standards such as the 5G Security toolbox and the Network and Information Security 2 Directive. We continue to monitor the forthcoming EU Cyber Resilience Act which aims to ensure that all digital products and services fulfil the same security requirements.

The US Securities and Exchange Commission ('SEC') introduced new cyber security incident disclosure and periodic reporting requirements in December 2023. We have updated our incident management process to include the relevant disclosure steps should a material incident occur; this is described in the Cyber Operations and Incidents section. Where applicable we have expanded these cyber security disclosures in response to the new reporting requirements.

Note:
1. Includes Vodafone Italy and Vodafone Spain.

# Operating model

## Our approach to cyber security

We have implemented a globally consistent cyber security operating model that is based on the leading industry security standards published by the US National Institute of Standards and Technology ('NIST'). The model is designed to reduce risk by constantly identifying threats, protecting, defending and improving our security. We operate cyber capabilities with an in-house international team of over 900[1] employees.

We augment our internal capabilities where necessary with third-party specialist technical expertise, such as digital forensics, red teaming and penetration testing. We use specialist resources to perform testing of our telecommunications networks. We also use qualified external resources to help during the implementation of change and improvement projects. Our scale means we benefit from global collaboration, technology sharing and deep expertise, and ultimately have greater visibility of emerging threats. An example would be our global security operations centre which takes inputs and telemetry from all the markets where we operate.

### Cyber security function

| Team | Responsibilities |
|---|---|
| **Governance, Risk and Control** | – Cyber risk framework and management across the Group.<br>– Define and track adoption of controls and procedures, and measure effectiveness.<br>– Identify and reduce supplier cyber risk. |
| **Strategy and Secure by Design** | – Define cyber strategy aligned to technology and Company strategies.<br>– Products, services and internal systems are secure by design. |
| **Cyber Prevent** | – Engineer, deliver and operate global security platforms, driving continuous improvement. |
| **Cyber Defence** | – Perform threat intelligence and security testing. Detect events and attacks through 24/7 monitoring.<br>– Respond to events and incidents to minimise the impact to business and customers. |
| **Local Market Teams** | – Responsible for managing and embedding cyber security in our local markets, including meeting local cyber regulatory and compliance requirements. |

Our approach to cyber security is summarised in the following diagram and the accompanying video linked below. In the video, cyber security experts from across teams in the cyber security function explain our approach across the lifecycle: identify, protect, detect, respond, recover and govern.

Scan or click to watch our cyber security experts summarise our approach to cyber security:
**investors.vodafone.com/videos**

# Operating model continued

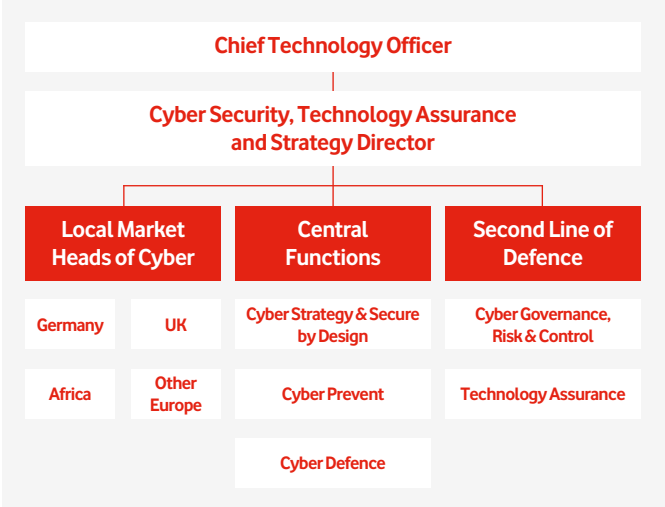
## Governance

### Management

The Chief Technology Officer ('CTO') and Chief Network Officer are the Executive Committee members accountable for managing the risks associated with cyber threats and information security. The Cyber Security, Technology Assurance and Technology Strategy ('CTAS') Director is responsible for managing and overseeing cyber security across Vodafone and reports to the Chief Technology Officer.

The Chief Technology Officer has been at Vodafone since 2009. During that time he has held positions in Vodafone Business Product Management and Technology, has been UK CTO and since 2021 the Chief Digital & Information Officer leading an integrated Europe-wide technology team.

Within the cyber security organisation, led by the CTAS Director, we have heads of global cyber security functions, local markets and regional cyber security leaders. This global leadership team is responsible for directing, managing and reducing cyber risk across Vodafone. Market and regional cyber security leaders are also part of their local management teams, with a dotted matrix reporting line to local chief information officers.




The CTAS Director has led cyber security in Vodafone since 2015. Prior to joining Vodafone, the CTAS Director was chief security officer at a large UK bank, after previously holding security and technology audit leadership roles in financial services and the UK postal service. The CTAS Director is an independent advisor for a large UK retail company, a member of the UK Cabinet Office National Cyber Advisory Board and holds several other industry advisory and committee roles. Our broader cyber leadership team has significant cyber security and technology risk experience across business sectors including telecommunications, financial services and professional services.

The cyber security leadership team reviews detailed metrics monthly covering security controls status, updates about the threat landscape, and specific key risk indicators ('KRIs') for our most important controls. Examples of KRIs include results of independent network testing by third parties, vulnerability management, patching, hardening and endpoint security status, and incident metrics. Internal reporting provides a detailed view of progress and risk reduction. If markets are consistently not achieving targets, they are expected to have plans in place to recover.

Quarterly summary management reporting is provided to the technology leadership team and Executive Committee. This is supplemented by monthly control status reports which track targets and are discussed in regular meetings with local market leadership teams.

The top level Cyber and Information Security policy is approved annually by the CTO. To provide functional governance, we have a quarterly Cyber Risk Council meeting, chaired by the Head of Cyber Governance Risk and Control, and attended by the CTAS Director, the CTAS leadership team and cyber security leaders from each market. The meeting reviews and approves detailed cyber policies and standards, monitors cyber risk and threat, and oversees key strategic programmes.

Cyber security risk is also reported to and monitored by more senior committees including the Technology and Audit and Risk Committee, chaired by Internal Audit and the Vodafone Group Risk and Compliance committee, chaired by the Chief Financial Officer ('CFO'). The CTAS Director attends both of those committees to provide updates as required.

### Board

The Board Audit and Risk Committee ('ARC') is the responsible committee for the oversight of risks from cyber security threats. The Committee receives updates from Internal Audit throughout the year. The Line of Sight report documents the risk tolerance, risk position and mitigating actions for each principal risk of the company, including cyber threat. This is presented and reviewed annually.

In addition, the Committee reviews cyber risk based on a paper and presentation from the CTO and CTAS Director. The report collates the data that covers all local markets' security status. The paper also typically includes threat landscape, incidents, security position, residual risk, strategy and programme progress across the Company. The most recent update was provided in March 2024.

The Chair of the Board's Audit and Risk Committee is the Senior Independent Director of the Board. A former CEO at a UK financial services company, he has significant experience of overseeing technology and cyber issues.

Click or scan to watch our Chair talk about the importance of cyber security during a Board site visit: **investors.vodafone.com/videos**

Scan or click to watch the chair of the Audit and Risk Committee talk about cyber security: **investors.vodafone.com/videos**

Click to read more about the Audit and Risk Committee's oversight of cyber security on pages 89 to 94 of our FY24 Annual Report: **vodafone.com/ar2024**

# Culture, training & awareness

## Training and awareness

Our cyber security awareness approach is to educate our employees to protect themselves and our customers from cyber threats. Cyber security training is mandatory as part of our Doing What's Right programme. The training module is designed by the cyber security team to inform employees of key threats and how to avoid them. The cyber leadership team are actively involved in shaping the approach and in specific employee communication. The corporate security function lead on all employee security training and they deliver the programme and materials. Mandatory training runs every other year with a short refresher and knowledge check in the intermediate year. If the knowledge check is failed, the employees are required to retake the full cyber security training module. During the year we launched a training manual for contractors, so they also receive the same level of awareness. Training on cyber security is also included in our induction process for new employees. We track completion rates to ensure every employee completes mandatory training when assigned.

Click to read more about our approach to mandatory Doing What's Right training on page 44 of our FY24 Annual Report: **vodafone.com/ar2024**

Cyber security training is reinforced by regular digital communications delivered via our internal social media platform, through videos and webinars. We respond to threats with specific targeted advice, such as the use of multi-factor authentication and reminders to not share credentials.

We perform phishing simulations across all markets and functions to raise awareness and train employees. We target at least two exercises per market or function per year. We also run multi-market simulations to allow us to compare responses consistently – in the most recent exercise we sent over 100,000[1] emails to nine[1] European markets and Group functions. Those who click on the link in the phishing message or share their credentials receive immediate training. We are now rolling out this multi-market approach to our African markets.

We also provided focused training for our Executive Committee. This year, we covered social engineering threats, use of social media, travel to high-risk countries, using devices securely and how to share confidential information safely. The training materials were cascaded to their teams by ExCo members.

We have continued to undertake incident simulations for local executive committees, most recently for Greece. The simulations provide CEOs and their teams a realistic and tailored experience of managing a cyber incident and exercising their responsibilities in accordance with our common approach.

## Growing our skills

We enable employees in our cyber teams to maintain and grow their skills to better protect our customers. Our company learning platform hosts cyber training on technical topics, platforms and frameworks. Employees can study towards recognised information security and cyber certifications aligned to their learning plans.

Since 2020 we have organised twice yearly cyber connect events for our entire global cyber security team. The events include a recap of our strategy and achievements, messages from senior leadership, external industry speakers, collaborative breakout groups and technical track sessions to learn about cyber topics and best practice. We use technology to enable a hybrid experience with some attending in offices and some remote.

## The Cyber Code

The Vodafone Cyber Code has been designed to simplify and explain basic security controls and procedures to all employees. The Cyber Code is embedded in our Code of Conduct and is the cornerstone of how we expect all employees to behave when it comes to best practice in cyber security. It consists of seven areas where employees must follow good security practice.

## Our Cyber Code

The Vodafone Cyber Code has been designed to simplify and explain the basic security controls to all employees. Embedded in our Code of Conduct, the Cyber Code is the cornerstone of how we expect all employees to behave when It comes to best practise in cyber security.

**ALWAYS** use multi-factor authentication for remote systems that hold sensitive information.

**NEVER** allow unsupported end of life systems in Vodafone infrastructure, or release unsecured products or services.

**ALWAYS** apply the latest security patches, close critical and high vulnerabilities and configure systems securely.

**NEVER** click on links or download without knowing who it is from. Report suspicious behaviour.

**ALWAYS** remove access when staff change roles or leave Vodafone. Secure privileged access and only use it for privileged tasks.

**NEVER** share or reuse your passwords. Longer is stronger.

**ALWAYS** classify, label and protect information you work with.

Click to read more about Vodafone's Cyber Code in our Code of Conduct: **vodafone.com/code-of-conduct**

Note:
1. Includes Vodafone Italy and Vodafone Spain.

# Threats and incidents

## Threat landscape and intelligence

An important part of our operating model is to gather intelligence and insights about threats. The cyber threat landscape continues to be volatile across all sectors, with wide-ranging threat actors. Our cyber security team use industry and external analysis to help shape our controls and procedures, and drive actions. When specific vendor or new high impact vulnerabilities are reported, we drive global remediation across Vodafone.

- Geopolitical instability, conflict and tensions often lead to an increase in cyber threats from state-backed and criminal threat actors. This can lead to disruption, data theft and integrity compromise. Cross-industry and government collaboration is vital.
- Ransomware and data extortion attacks are common to companies of all sizes. The threat is increasing. Based on public reporting, some companies are paying ransoms, aggravating the threat.
- Attackers are increasingly trying to log in, rather than hack in. As such, social engineering methods are a common means for attackers to gain access. Emerging technologies such as AI will enhance techniques such as voice phishing and deep fakes. Harvested credentials continue to be sought and shared by threat actors. Attackers can target executives following media announcements and public reporting.
- The speed of vulnerability exploitation is very fast, with a trend for targeting internet-facing software.
- In 2023, the European Commission highlighted the number of supply chain attacks in Europe has tripled. Supplier attacks against all sectors are likely to increase in the coming year.

We anticipate threats will continue from existing sources, as well as evolving in new technology areas such as artificial intelligence and quantum computing.

## Cyber operations and incidents

As a global connectivity provider, we see a range of cyber threats. We use our layers of controls to identify, block and mitigate threats and reduce business or customer impact. Our global security operations capability handles trillions of events and logs from sensors across our footprint, detecting potential threats and events. Low severity issues are dealt with quickly, for example by malware containment or isolating an individual device. More significant events are triaged to our 24/7 incident management and response team. We operate a single global team and capability.

Where a security incident occurs, we have a consistent incident management framework to manage our response and recovery. The focus of our incident responders is always fast risk mitigation and customer security.

In the event of a cyber breach, disclosure is made to the relevant authorities in line with local and global regulations and laws and a risk assessment considering the impact on customers. This may include law enforcement as well as regulators. The European Union's GDPR provides a framework for notifying customers in the event there is a loss of customer data because of a data breach, and this framework is a baseline across all our markets. Our data privacy officers are a key part of the response where incidents impact personal data. We will also notify the SEC if an incident is deemed material.

We classify security incidents on a scale according to severity, measured by potential business and customer impact. The highest severity category of event is called Severity 0 down to the lowest Severity 4. Severity 0 corresponds to a significant data breach or loss of service caused by the incident. If a Severity 0 incident occurs, we notify the Executive Committee, the Board and external auditors and provide regular updates. A crisis group is formed composed of relevant senior management who oversee the response.

SEC requirements have been incorporated into our incident management process. In the event of a Severity 0 incident, the Disclosure Committee (composed of the CFO and General Counsel) would decide if a UK market disclosure is necessary for materiality reasons, that would also trigger disclosure to the SEC.

In the past two financial years, no incidents have been Severity 0. In FY22 we experienced one Severity 0 in Vodafone Portugal in February 2022 and in FY21 we experienced one Severity 0 incident at Italy Ho. Mobile in December 2020. Details of these two previous disclosures are in our FY23 Cyber Security Factsheet. These incidents did not have a material impact on the Company's business strategy, results of operations or financial condition.

Whilst overall incident volumes have remained stable, a higher proportion of these are at suppliers and third parties. In FY24, 55% of severity 1 and 2 incidents were related to our suppliers and third parties (FY23; 47%). We contractually require our suppliers to report incidents and we track and manage the incidents using the same framework as we do for internal events. In two cases in this financial year, our team helped a supplier recover services after a ransomware attack. Neither of these incidents were material to Vodafone's business strategy, results of operations or financial condition.

When incidents are closed, we complete a post-incident review to learn the lessons from the incident, including the root cause and any improvements needed.

Cyber insurance is an important part of our risk management and litigation approach. Vodafone holds cyber liability insurance alongside business interruption and professional indemnity policies. Should a serious cyber event occur, we could recover the costs in whole or in part through these policies.

Click to read more about how we manage risks from technology disruptions in our SASB disclosure: **investors.vodafone.com/sasb**

# Compliance with Securities and Exchange Commission cyber security disclosure requirements

The United States Securities and Exchange Commission ('SEC') introduced new cyber security reporting requirements in December 2023. We have adopted the requirements in our processes for assessing, identifying, and managing material risks from cyber security threats throughout this report. Many of the requirements were covered in our previous cyber security reporting, however this content has been moved into this report. Additionally, we have cross-referenced our disclosures to the new SEC requirements in this table.

| SEC disclosure requirement | Disclosure | Page |
|---|---|---|
| Risk management & strategy (Form 20-F Item 16K (b)) | | |
| 1. Describe the registrant's processes for assessing, identifying, and managing material risks from cyber security threats: | Risk management > Identification of vulnerabilities and risks | Page 4 |
| i. Whether any such processes have been integrated into the registrant's overall risk management system or processes | | |
| ii. Whether the registrant engages assessors, consultants, auditors or other third parties in connection with any such processes, and; | Risk management > Risk and control approach > Assurance | Page 5 |
| iii. Whether the registrant has processes to oversee and identify such risks from cyber security threats associated with its use of any third-party service provider | Risk management > Risk and control approach > Supply chain | Page 5 |
| 2. Describe whether any risks from cyber security threats, including as a result of any previous cyber security incidents, have materially affected or are reasonably likely to materially affect the registrant, including its business strategy, results of operations, or financial condition | Threats and incidents > Cyber operations and incidents | Page 9 |
| Governance (Form 20-F Item 16K(c)) | | |
| 3. Describe the board's oversight of risks from cyber security threats. If applicable, identify any Board committee or subcommittee responsible for the oversight of risks from cybersecurity threats and describe the process by which the board or such committee is informed about the risks | Operating Model > Governance > Board | Page 7 |
| 4. Describe management's role in assessing and managing material risks from cyber security threats: | Operating model > Governance > Management | Page 7 |
| i. Whether and which management positions or committees are responsible for assessing and managing such risks, and the relevant experience of such persons or members in such detail as necessary to fully describe the nature of the expertise | | |
| ii. The processes by which such persons or committees are informed about and monitor the prevention, detection, mitigation and remediation of cyber security incidents | | |
| iii. Whether such persons or committees report information about such risks to the board or a committee or subcommittee of the board | | |
| Material cyber security incidents (Form 6-K) | | |
| Information on material cyber security incidents that they disclose or otherwise publicize in a foreign jurisdiction, to any stock exchange, or to security holders | There have been no such incidents in the current or prior financial years. | |

Together we can

**Vodafone Group Plc**
Vodafone House
The Connection
Newbury
Berkshire
RG14 2FN
England

Registered in England No. 1833679

Telephone +44 (0)1635 33251

**vodafone.com**

## Contact details

**Investor Relations**
ir@vodafone.co.uk
vodafone.com/investor

**Media Relations**
vodafone.com/news/contact-us

**Sustainability**
vodafone.com/sustainability

**Online Annual Report**
vodafone.com/ar2024